Software Security in Legacy Systems

Carl Weber, Cigital, Inc. [vita[1]]
Craig Miller, Cigital, Inc.

2006-12-14

Much of the emphasis in your organization is undoubtedly on new systems work. You certainly have well-developed processes for building new systems, and you carefully track new software development activity. This attention is appropriate, since it is not simple to install new software, test it fully, and deploy it throughout the organization.

Typically, though, a large portion of your code base lies in the legacy systems. Not just the major systems, but a myriad of smaller systems in every corner of the organization. These legacy systems do the hard, day-to-day work of your organization. Further, a considerable portion of your systems development work is directed at maintenance and extension of these existing systems, though these smaller projects are often done without benefit of the rigorous methods, independent review, and management attention devoted to new systems work. The result is increased performance risk and greater security risk.

Discussions elsewhere on the Build Security In web site address developing new systems. Their basic message is that you should design and code systems with security in mind. Systems constructed in this way are inherently more secure because they minimize the design flaws and coding errors that attackers can exploit.

But your existing legacy systems undoubtedly contain the same sorts of security flaws and bugs that attackers look for and that you work so hard to root out and contain in new systems. How should you address these in legacy systems?

This content area offers two articles to help answer this question.

- Assessing Security Risk in Legacy Systems[2] offers a simple approach for determining the level of risk posed by these legacy systems and for identifying the systems that deserve immediate attention.
- Security Considerations in Managing COTS Software[3] addresses security issues in commercial off-the-shelf software products that often compose a major portion of the legacy systems within an organization.

Cigital, Inc. Copyright

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

1. http://buildsecurityin.us-cert.gov/bsi/about_us/authors/640-BSI.html (Weber, Carl C.)
1. mailto:copyright@cigital.com